GARY M. RESTAINO
United States Attorney
District of Arizona

AMY C. CHANG
Arizona State Bar No. 027566
Email: Amy.Chang@usdoj.gov
M. BRIDGET MINDER
Arizona State Bar No. 023356
Email: Bridget.Minder@usdoj.gov
Assistant United States Attorneys
Two Renaissance Square
40 N. Central Ave., Suite 1800
Phoenix, Arizona 85004
Telephone: 602-514-7500
Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

United States of America, Plaintiff, vs. Jordan Dave Persad, Defendant.	**No. CR-23-00680-PHX-DJH** **UNITED STATES' SENTENCING MEMORANDUM**

For nearly eighteen months, defendant and his co-conspirators hacked into the victims' email accounts, hijacked their cell phone numbers, and gained unauthorized access to their online cryptocurrency accounts. As a result of this scheme, often referred to as "SIM swapping," defendant and his co-conspirators stole close to $1 million worth of cryptocurrency from dozens of victims, including approximately $30,000 from a victim in Arizona. Defendant's conduct caused substantial financial hardship to these victims, several of whom lost their life's savings. Defendant and his co-conspirators then divided these stolen funds amongst themselves, with defendant keeping around $475,000. Investigators recovered some of these funds when they searched his home; however, defendant spent a portion of the stolen funds on designer clothes, luxury watches, and other expenses.

For this conduct, the government recommends a 30-month sentence, followed by three years of supervised release and the repayment of restitution to victims. The government believes such a sentence—which is below the low-end of the recommended Sentencing Guidelines range—appropriately balances the seriousness of the offense and its impact on victims with defendant's history and characteristics. The sentence also adequately addresses public policy concerns, including the need to promote respect for the law, provide just punishment, and afford adequate deterrence.

The Guidelines Range and PSR

The Presentence Investigation Report (PSR, doc. 21), calculates an offense level of 21 and a criminal history category of I, which corresponds to a Guidelines range of 37-46 months in custody. The government agrees with the Guidelines calculation. The PSR recommends a sentence of 37 months, followed by three years of supervised release, and restitution in the amount of at least $941,587[1] to victims. (PSR, p. 20.)

The § 3553(a) Factors

After considering the nature and circumstances of the offense, defendant's history and characteristics, and the public policy factors, the government respectfully requests a two-level downward variance and recommends a sentence of 30 months in custody. While this sentence falls below the recommended Guidelines range, the government believes 30 months in custody—coupled with a term of supervised release and a significant restitution obligation—is sufficient but not greater than necessary to comply with the § 3553(a) factors.

I. The nature and circumstances of the offense

As detailed in the PSR, defendant's offense conduct was serious. Over the course of eighteen months, defendant engaged in a complex, multi-faceted computer intrusion scheme that had devastating financial and emotional effects on his victims. The offense conduct was not an isolated, one-time infraction. Rather, defendant choreographed a long-

[1] The restitution amount may change before sentencing, as additional victims may reach out to the Probation Office with information about their losses.

running, multi-step conspiracy to steal cryptocurrency from victims across the country, including in Arizona. (PSR ¶¶ 5-22.)

As part of the scheme, defendant bought and sold (and in some cases, re-sold) access logs containing tens of thousands of victim email addresses and passwords. While defendant bought and sold these logs to and from other online hackers and cybercriminals, he and his co-conspirators also used these logs as the starting point for identifying "targets" for their SIM swapping scheme. Defendant and his co-conspirators ran computer scripts against these access logs to identify potential victims who had online cryptocurrency accounts, sorting them into buckets based on the balances available in the victims' accounts. (PSR ¶¶ 9-10.)

Defendant and his co-conspirators then used the stolen credentials to access the victims' email accounts, gaining important information about the victims' personal lives that they could later exploit for social engineering purposes. During a forensic search of defendant's computer, investigators found he had entered close to 450 different email addresses into fields at various websites. (PSR ¶ 11.)

Once defendant and his co-conspirators hacked into the victims' email accounts, they then used various techniques to hijack the victims' phone numbers through a process generally referred to as "SIM swapping." In some cases, they hired an insider at a telephone company to effectuate the swap; in others, they posed as the victims and used social engineering techniques to convince an unwitting employee to complete the swap. Once the swap was completed, defendant and his co-conspirators effectively controlled the victims' cell phones, as any text messages intended for the victims would instead be routed to devices held by defendant or his colleagues. (PSR ¶ 12.)

With control over both the victims' text messages and emails, defendant and his co-conspirators were then able to hack into the victims' cryptocurrency accounts by resetting the account passwords and entering the multi-factor authentication codes received by the swapped telephone. Once they gained access to these cryptocurrency accounts, defendant and his co-conspirators "cashed out" by withdrawing the victims' funds and transferring

them into cryptocurrency wallets they controlled. They then laundered the stolen cryptocurrency through mixing services and currency exchanges to conceal the source of the funds, ultimately dividing the stolen cryptocurrency amongst themselves. (PSR ¶¶ 13-16.)

This complex scheme involved several co-conspirators, each of whom played specific roles: for example, one person might be responsible for identifying targets or victims; one person might be in charge of facilitating the SIM swap; one person might be holding the swapped phone; and another might be responsible for cashing out the cryptocurrency account. Over the course of the scheme, defendant played nearly all of these roles—as he grew in experience, he became the coordinator responsible for orchestrating the entire scheme. (PSR ¶ 17.)

All told, defendant's SIM swapping scheme resulted in close to $1 million in victim losses, with defendant keeping nearly half of that for himself.[2] (PSR ¶¶ 20-22; Doc. 5 at 8.) The victims, the majority of whom lost tens of thousands of dollars, have described the devastating impact of the crime, both financially and emotionally. Several have noted that the scheme robbed them of their life's savings, as well as a sense of security, resulting in anxiety, depression, and other health concerns. (PSR ¶¶ 21-47.)

II. Defendant's history and characteristics

Although the nature and circumstances of the offense are serious, defendant's history and characteristics are to some extent mitigating. At twenty years old, this is defendant's first offense. (PSR ¶¶ 64-70.) His youth and lack of criminal history suggest that the underlying conduct may have been fueled at least in part by heedless immaturity.

---

[2] As explained in the PSR, these figures represent a reasonable estimate of the financial impact of the scheme. In determining the loss amount, agents identified the individuals whose email addresses or other credentials were sent by defendant to co-conspirators via chat messages or were entered by defendant into fields at various websites. From this group of more than 450 potential victims, agents then identified around 25 victims who submitted complaints to the FBI that they had been the victim of cryptocurrency theft. Thus, the list of identified victims is based on the individuals who reported thefts to FBI, suggesting that many other individuals may have suffered losses but have not reported them.

And although the government agrees with the PSR that a downward departure under U.S.S.G. § 5H1.1 (Age) is not warranted given the sophistication and long-running nature of the scheme, the government believes defendant's youth can and should be taken into account for mitigation purposes.

In addition, defendant's conduct over the course of the investigation and prosecution of the offense has been positive. He has remained in regular communication with his attorney and abided by his release conditions. He also voluntarily traveled to Phoenix to meet with the government and provided information about his offense. By entering a pre-indictment resolution, accepting responsibility for his actions, and disclaiming any interest in the stolen cryptocurrency seized at his residence, he has helped the government conserve investigative time and resources. The government believes that these actions—when coupled with his youth and lack of criminal history—warrant a two-level downward variance from the Guidelines.

III. Public policy factors

The government further believes a 30-month sentence is sufficient but not greater than necessary to satisfy the public policy factors set forth in 18 U.S.C. § 3553(a)(2). A two-level downward variance accounts for defendant's youth, acceptance of responsibility, and willingness to resolve the case quickly and efficiently. A 30-month sentence is also significant enough to deter future crimes by defendant and provide general deterrence to other would-be fraudsters operating online. Many of these cybercriminals appear to have a false sense that because their crimes occur on the internet, behind the protection and pseudonymity of online monikers, obfuscated IP addresses, and digital currency, the crimes do not have real and tangible consequences. As is made clear in the dozens of victim impact statements submitted to the Court, this is simply not true. The government therefore believes a 30-month sentence should be imposed, as such a sentence appropriately balances the need to deter similar crimes, protect the public, promote respect for the law, and to provide just punishment.

//

Conclusion

For the foregoing reasons, the government respectfully asks the Court to impose a sentence of 30 months' imprisonment, followed by three years' supervised release, and restitution as specified in the PSR.

Respectfully submitted this 10th day of October, 2023.

GARY M. RESTAINO
United States Attorney
District of Arizona

s/ Amy Chang
AMY C. CHANG
M. BRIDGET MINDER
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that on October 10, 2023, I electronically transmitted the attached document to the Clerk's Office using the CM/ECF System for filing a copy to the following CM/ECF registrants:

Mark J O'Brien
Attorney for Defendant

By: s/ *Alexandria Gaulin*
U.S. Attorney's Office